خبر صحافي للنشر
1 فبراير 2015

تقرير الأمن الإلكتروني السنوي من سيسكو يكشف عن توسع الفجوة مابين الاعتقاد السائد وواقع التهديدات الإلكترونية

سيسكو تقدم دليلها الأمني ليكون أساساً لمؤسسات الشرق الأوسط لفهم تحديات الهجمات الأمنية المعاصرة والاستجابة لها بفعالية

دبي، الإمارات العربية المتحدة
كشف تقرير سيسكو السنوي للأمن الإلكتروني لعام 2015، والذي نشر اليوم ويبحث في توجهات استقصاء التهديدات والأمن الإلكتروني، أن على المؤسسات تبني منهجية تعاونية شاملة لحمايتها من الهجمات الإلكترونية. فقد أصبح المهاجمون أكثر احترافية في استغلال الثغرات الأمنية وتجنب الاكتشاف وتمويه الأنشطة الضارة. أما الدفاع المتمثل في فرق الأمن فعليه أن يحسن أساليبه باستمرار في حماية المؤسسة من تلك الهجمات الإلكترونية متزايدة التعقيد. ويتضاعف التعقيد بسبب الدوافع السياسية لدى بعض المهاجمين، والتضارب في متطلبات تحديد مواقع البيانات وسيادة الدول.

دليل سيسكو للأمن الإلكتروني

تخلص نتائج التقرير إلى أن الوقت قد حان لتتولى مجالس الإدارة دورها في تحديد الأولويات الأمنية والتوقعات في هذا الجانب. ويمكن لدليل سيسكو، وهو مجموعة من المبادئ الأمنية التي تشكل قواعد أساسية لتحقيق الأمن، مساعدة المدراء وفرق الأمن والمستخدمين في المؤسسة لتحقيق فهم أوسع يمكنهم من التجاوب مع تحديات الأمن الإلكتروني في عالمنا المعاصر. ويمكن اعتباره أساساً للمؤسسات التي تسعى إلى ان تصبح أكثر ديناميكية في منهج تعاملها مع إجراءات الأمن الافتراضي والتكيف مع الابتكارات بشكل تتفوق فيه على خصومها. ومن أهم هذه المبادئ:

1. على الأمن أن يدعم الأعمال
2. يجب أن يعمل الأمن بالتزامن مع البنية القائمة وأن يكون قابلاً للاستخدام.

3. يجب أن يتسم الأمن بالشفافية وتقديم المعلومات
4. يجب أن يتيح الأمن إمكانات الرؤية والتصرف الملائم
5. يجب اعتبار الأمن بأنه "مشكلة شخصية"

المهاجمون:

يعمل المهاجمون عبر الإنترنت على تعزيز أساليبهم وترسيخ مهمتهم للقيام بالهجمات الأمنية وجعل الكشف عنها أكثر صعوبة. وتتمثل أهم ثلاث توجهات كشفت عنها سيسكو في مجال التهديدات ما يلي:

- **البريد التطفلي بكميات بسيطة:** وهو توجد جديد ومفضل للهجوم بحيث يرسل المهاجمون أعدادا قليلة من رسائل البريد التطفلي من عدد كبير من عناوين بروتوكول الإنترنت لتجنب اكتشافهم.
- **نقاط الاستغلال المخبأة في مواقع عادية:** تتمكن الشركات الأمنية من تفكيك ادوات استغلال الإنترنت بسرعة، ولهذا أصبح المهاجمون يستخدمون وسائل اخرى أقل شيوعا للنجاح في هجماتهم، وهو نموذج مستدام للأعمال لأنه لا يستقطب اهتماماً كبيراً.
- **الدمج بين البرمجيات الضارة:** عرفت برامج Flash وJavaScript بكونها غير آمنة بحد ذاتها، ولكن التقدم في مجال الأمن دفع المهاجمين إلى الدمج بين أضعف النقاط في كليهما. يمكن الآن للبرمجيات المضرة بتقنيات Flash التفاعل مع برمجيات JavaScript وإرسال الثغرة في ملفين لكليهما. وهذا النوع من التهديدات يصعب اكتشافه.

المستخدمون:

المستخدمون عالقون في المنتصف. فإلى جانب كونهم الهدف الفعلي، فإنهم يساعدون المهاجمين الإلكترونيين دون قصد أو علم. خلال عام 2014، كشفت وحدة أبحاث الهجمات الإلكترونية أن المهاجمين نقلوا تركيزهم من الخوادم وأنظمة التشغيل لأن المزيد من المستخدمين يقومون بتنزيل ملفاتهم من مواقع تمت مهاجمتها، مما سبب زيادة بنسبة 280% في هجمات سيلفرلايت وارتفاع بنسبة 250% في هجمات البريد التطفلي والإعلان الإغراقي.

المدافعون:

أظهرت دراسة سيسكو القياسية للتهديدات، والتي استطلعت آراء عدد من مدراء أمن المعلومات ومسؤولي عمليات الأمن في 1700 شركة حول العالم، وجود ثغرة تزداد اتساعاً بين نية المدافع وتصرفاته. وبشكل أوضح فإن الدراسة تبين أن 75 بالمائة من مدراء أمن المعلومات يرون أن أدواتهم الأمنية فعالة جدا أو فائقة الفعالية، بينما قال أقل من 50 بالمائة من المشاركين في الدراسة أنهم يستخدمون الأدوات المعيارية،كالترقيع والتكوين، للمساعدة في تجنب

الاختراق الأمني وضمان استعمال أحدث الإصدارات. كانت Heartbleed هي نقطة الضعف الأبرز العام الماضي، ولكن 56% من إصدارات OpenSSL عمرها اكثر من أربعة أعوام ونصف. وهذا مؤشر قوي على أن فرق الأمن لا تقوم بتحديث الإصدارات وسد الثغرات.

وفيما يعتقد العديد من المتواجدين في جانب الدفاع أن عملياتهم الأمنية في أفضل مستوياتها، وأن الأدوات الأمنية فعالة جدا، فإن الجاهزية الأمنية في الواقع تحتاج إلى الكثير من التحسين.

للحصول على نسخة كاملة من تقرير سيسكو السنوي للأبحاث، الرجاء الاطلاع على الرابط
.www.cisco.com/go/asr2015

نبذة عن التقرير

يعتبر تقرير سيسكو السنوي للأمن 2015 واحداً من أبرز التقارير الأمنية الهامة، حيث يبين أحدث ما توصل إليه خبراء الأمن لدى سيسكو في مجال الأمن ليقدموا للعاملين في المجال لمحة هامة عن التوجهات وأهم النتائج المتعلقة بالأمن للعام 2015. كما يسلط التقرير الضوء على نتائج أحدث دراسة أجرتها سيسكو لمعايير القدرات الأمنية، وهي دراسة تبحث في الوضع الأمني للمؤسسات وأفكارها المسبقة حول مدى جاهزيتها للدفاع عن نفسها أمام الهجمات الإلكترونية. ويناقش التقرير كذلك عدداً من المواضيع، منها التوجهات السياسية الجغرافية والتطورات العالمية في مجال تحديد موقع البيانات وأهمية جعل الأمن الإلكتروني موضوعاً أساسياً على مستوى المؤسسة ككل.

وفي تعليقه على التقرير قال ربيع دبّوسي، المدير العام لدى سيسكو الإمارات : "أصبح الأمن الآن مسؤولية الجميع في المؤسسة – من مجلس الإدارة وحتى المستخدمين من الأفراد. فقادة الأمن والعاملون في المجال بحاجة إلى دعم الأعمال بالكامل لمكافحة المهاجمين الذين تزداد خبرتهم في استغلال الثغرات وإخفاء هجماتهم بحرفية تامة. ولحماية المؤسسات من تلك الهجمات المستمرة، فإن على مدراء تقنية المعلومات الحرص على توفير الأدوات اللازمة للفريق وتزويده بالرؤية الصحيحة لوضع استراتيجية أمنية ملائمة، إلى جانب تثقيف المستخدمين للمساعدة في تأكيد سلامتهم وسلامة أعمالهم."

واختتم حديثه بالقول: "أصبح المهاجمون اكثر خبرة واحترافية في استغلال الثغرات الأمنية. ففي أي لحظة يمكننا أن نتوقع وجود استغلال فعلي لنقاط ضعف خطرة بنسبة تضاهي واحداً بالمائة – بينما لا تزال 56% من إصدارات Open SSL معرّضة لهجمات Heartbleed. على الرغم من ذلك نرى ان أقل من نصف فرق الأمن المشاركة في الدراسة تستعمل الأدوات القياسية، كالترقيع وإدارة التكوين للمساعدة في منع الاختراق الأمني. فحتى مع توفر التقنيات الأمنية الرائدة لا زال علينا الحرص على التميز في العمليات من أجل حماية المؤسسات والمستخدمين من الهجمات متزايدة التعقيد.

-انتهى-

لمزيد من المعلومات

أخبار «سيسكو» بمنطقة الشرق الأوسط

http://www.cisco.com/web/ME/about/news/index.html

معلومات عن «سيسكو»

http://www.cisco.com

نبذة عن شركة سيسكو:

تعمل شركة "سيسكو"، الرائدة عالمياً في مجال تقنية المعلومات والمدرجة في بورصة الأوراق المالية "ناسداك" تحت الرمز (NASDAQ: CSCO) ، على مساعدة الشركات في استغلال الفرص المستقبلية من خلال إثبات أن تحقيق الإنجازات المذهلة يكون عبر تمكين الاتصال الشبكي لما هو غير متصل. لمتابعة أخبار سيسكو، الرجاء زيارة http://thenetwork.cisco.com .

###